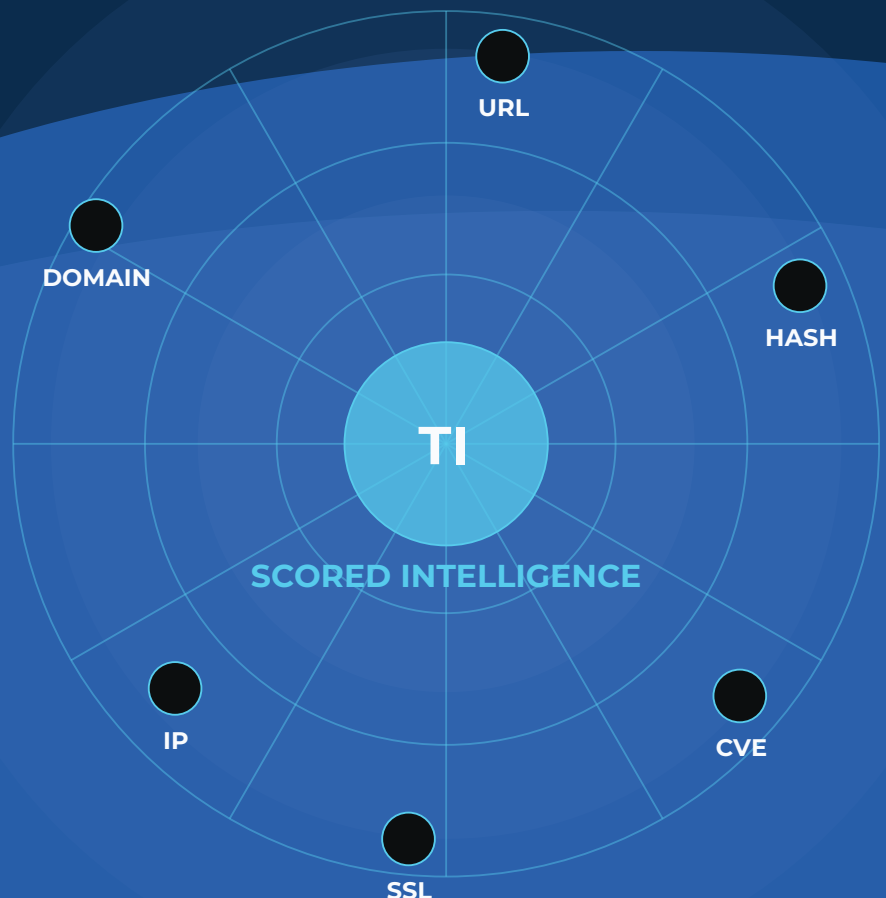




See your digital footprint before attackers do.

Ornis Recon is a multi-tenant CTI platform that transforms internet-facing assets, exposures, leaked credentials, vulnerabilities and threat indicators into scored, actionable intelligence. It brings external attack surface visibility, IoC analysis, relationship graphs, reporting and customer-specific intelligence services together in one platform.



From externally visible risk to organisation-specific intelligence

Internet-facing assets change continuously. Ornis Recon helps security teams identify and prioritise the threats relevant to their organisation.

Where does hidden risk emerge?

- Forgotten subdomains and internet-facing services
- Expired certificates and outdated technologies
- Corporate accounts found in leak sources
- Indicator and reputation data fragmented across multiple tools
- Manual reports prepared separately for every customer
- Custom integrations built to transfer intelligence into security tools

What does ornis recon change?

- Presents each organisation with its own digital risk view
- Explains source confidence, recency and cross-validation
- Links findings to assets, credentials, technologies and CVEs
- Automatically deactivates findings closed at the source
- Turns an investigation into a shareable report with one click

Intelligence workflow - current visibility in six steps

Every finding follows a traceable and auditable path from its source to the customer portal.

1. Discover

Continuously monitor assets, technologies and certificates.

2. Detect

Identify organisation-specific exposures, credentials, vulnerabilities and alerts.

3. Validate

Cross-check with multiple sources and MISP data.

4. Score

Enrich with a 0-10 TI score, reputation, location and ASN.

5. Correlate

Show links between assets, alerts, technologies, credentials and CVEs.

6. Deliver

Share through an isolated portal, reports and exports.

Scope

Each customer's own digital footprint

Isolated by organisation and permission scope.

Explainability

The source behind every score

Confidence, recency and validation remain visible.

Receny

A lifecycle for every finding

Records closed at the source are deactivated automatically.

Threat alerts

- ✓ Organisation-specific alerts, details and attachments
- ✓ Criticality, status, date and tag filters
- ✓ Asset/credential/indicator links
- ✓ Platform alert references
- ✓ Automatic deactivation and authorised history

External attack surface

- ✓ Domain, IP and service inventory
- ✓ Technology and version detection
- ✓ SSL/TLS certificate validity
- ✓ Asset-technology-CVE matching
- ✓ Automatic deactivation of removed assets

Exposures and credentials

- ✓ Open service, misconfiguration and leak
- ✓ Masked view of corporate accounts
- ✓ Account links to alerts and assets
- ✓ Authorised reveal and audit record
- ✓ Premium access control

Vulnerability intelligence

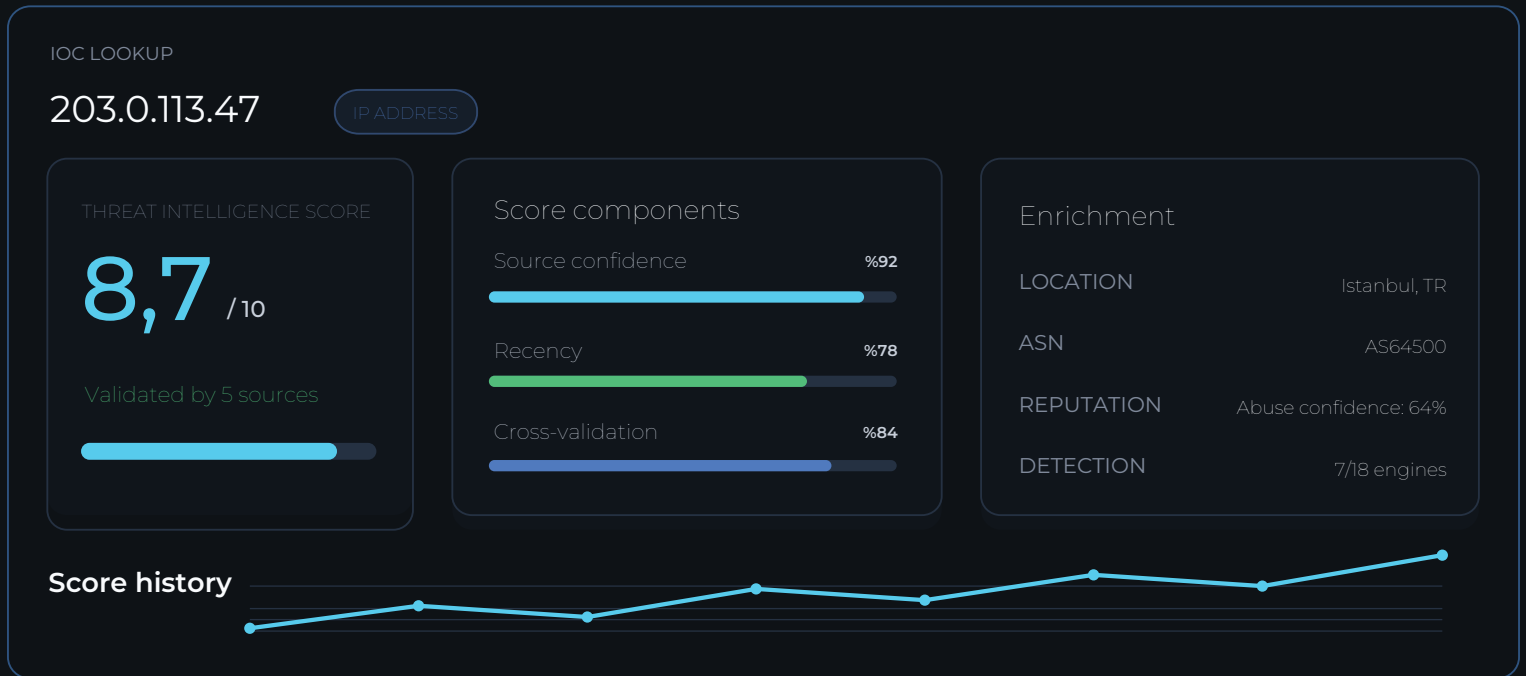
- ✓ CVEs matched to technologies and their details
- ✓ Affected asset and technology links
- ✓ Filterable vulnerability lists
- ✓ Excel export

Current and auditable record lifecycle

Alerts closed at the source and removed assets are deactivated automatically; historical records are retained by permission and screens remain current.

See the complete picture of an indicator on one screen

For an IP, domain, URL or hash, Ornis Recon applies a transparent scoring formula, enriches the result and stores it with its history.



Four layers that support analyst decisions



Exact-match search

Searches the indicator across all authorised intelligence sources.



Local geolocation

Generates location and ASN data without sending an external query.



Resilient querying

Cache and daily request budgets protect external service quotas.



Logging and quotas

Customer-based daily/weekly quotas; every query is audited.

Search and enrichment capabilities

Search and scoring

- ✓ Multi-engine detection score for IP, domain, URL and hash
- ✓ Exact-match search across all authorised sources
- ✓ Source confidence, explanatory badges, abuse confidence and report count
- ✓ Permanent storage of results with history

Enrichment and resilience

- ✓ Track score changes over time
- ✓ Enable or disable providers by organisation
- ✓ Protect quotas with cache and a daily request budget
- ✓ Continue searches when a service is unavailable
- ✓ Interactive 3D globe for location data

Ornis Recon correlates the external attack surface, threat alerts, leaked accounts and asset-matched vulnerabilities in one place. Its current, filterable record structure helps teams assess risk in the right context, prioritise it and turn it into customer-specific outputs.

[See assets](#) • [Analyse relationships](#) • [Prioritise risks](#) • [Accelerate action](#)

From the external attack surface to the relationship graph

Ornis Recon does more than inventory internet-facing assets; it links them to technologies, certificates, vulnerabilities, alerts and leaked credentials.

✓ Domain

Subdomains, organisation relationship and current inventory

✓ IP and service

Open ports and externally visible services

✓ Technology

Product, component and version detection

✓ Certificate

SSL/TLS validity and expiry tracking

✓ Vulnerability

CVE details; links to affected assets and technologies

✓ Exposure

Masked account linked to its related asset and alert

Investigation graph

Track links between assets, alerts, credentials, technologies and CVEs in one view.



Investigation and reporting

- Open a related finding instantly from any node
- Save an investigation and continue where you left off
- Live dashboards and charts based on organisation scope
- Global search and data-type-specific filters
- HTML/PDF reports with graph screenshots and attachments
- Excel export from filterable lists
- Web-based light and dark themes

Multi-source intelligence, one data model

Ornis Recon combines and validates its own detections, open-source MISP community intelligence and external reputation services in one platform.

Recon detections

The organisation's external surface

MISP

Standard and premium

Reputation services

Cross-validation

Synchronisation

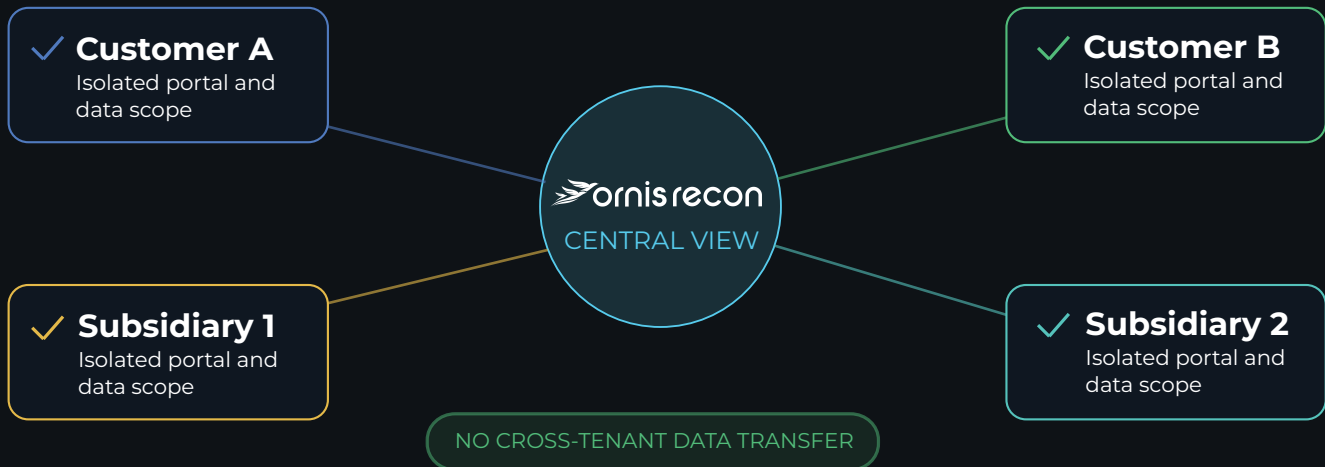
Scheduled / manual

Track progress in real time, cancel and resume; the number of sources validating the same indicator affects its score.

Each customer sees only their own intelligence

For MSSPs and multi-entity organisations, Ornis Recon maintains customer isolation across portals, searches, quotas, reporting and premium data access.

Multi-tenant intelligence architecture



Isolated portal

- ✓ Asset, alert, leaked account and CVE view
- ✓ The same isolation in the portal and IoC search
- ✓ No other customer's data is visible on any screen

Contracts and quotas

- ✓ Premium data only for contracted customers
- ✓ Customer-specific daily/weekly IoC search quota

Group view

- ✓ Subsidiaries and business units remain separate
- ✓ A consolidated risk view for the central team

History retention

- ✓ History remains when service is suspended
- ✓ Access is restricted without deleting records

Intelligence aligned with your brand

Your service remains visible instead of provider references; transformation rules preserve identity and relationship integrity.

Content transformation rules

- ✓ Apply find-and-replace before collected text is stored
- ✓ Exact word, regex and other match types
- ✓ Replace or remove matching content
- ✓ Automatically preserve identity, relationship and date fields
- ✓ Replace provider references with customer-facing brand language

Versioned and controlled application

- ✓ Manage rule sets with version control
- ✓ Preview the impact before applying rules to historical data
- ✓ Monitor application to historical data and cancel when needed
- ✓ Adapt customer-facing content to your brand language

Manage threat intelligence from one place

Dashboards, search, reporting, customer management and security controls come together in one web-based operations interface.

RECON OVERVIEW

ASSETS

2.481

ALARM

126

EXPOSURES

38

CVEs

594



● Critical	14
● High	37
● Monitored	75

Alert and asset management

Criticality, status, date and tag filters; global search and a current record lifecycle.

Reporting and sharing

Turn the investigation graph and attachments into HTML/PDF reports, and lists into Excel exports.

Sources and synchronisation

Manage providers by organisation; monitor scheduled or manual synchronisation.

Security and Data Privacy

Your service remains visible instead of provider references; transformation rules preserve identity and relationship integrity.

Runs on premises

- ✓ Customer intelligence never leaves for a third-party cloud
- ✓ Fully on-premises deployment

Identity and access

- ✓ Mandatory TOTP two-factor authentication
- ✓ CAPTCHA and IP-based brute-force protection
- ✓ Role- and organisation-scoped access for every screen and action

Data protection

- ✓ Leaked credentials and secrets are encrypted in the database
- ✓ Credentials are masked on screen
- ✓ Authorised reveal actions are audited

Audit and protocols

- ✓ Access records by user, IP and result
- ✓ TLS 1.2/1.3, CSP, HSTS and CSRF protection



See the intelligence portal you can offer your customers.

Monitor, validate and report the external risks affecting your organisation and customers on one platform. Request a demo to experience the isolated portal.

Experience Ornis Recon in your organisation's security operations.

Demo and further information:

ornis.com.tr

info@ornis.com · 0850 290 0 290

